The US-CERT Cyber Security Bulletin provides a summary of new and updated vulnerabilities, exploits, trends, and malicious code that have recently been openly reported. Information in the Cyber Security Bulletin is a compilation of open source and US-CERT vulnerability information. As such, the Cyber Security Bulletin includes information published by sources outside of US-CERT and *should **not** be considered the result of US-CERT analysis or as an official report of US-CERT*. Although this information does reflect open source reports, it is not an official description and should be used for informational purposes only. The intention of the Cyber Security Bulletin is to serve as a comprehensive directory of pertinent vulnerability reports, providing brief summaries and additional sources for further investigation.

Vulnerabilities

- Windows Operating Systems
  - AmbiCom Blue Neighbors Bluetooth Arbitrary Code Execution
  - AOL You've Got Pictures ActiveX Control Remote Buffer Overflow
  - ASPSurvey SQL Injection
  - BlogPHP SQL Injection
  - Check Point VPN-1 SecureClient Privilege Elevation
  - Computer Associates Unicenter Remote Control Denial of Service
  - CM3CMS SQL Injection
  - eStara Softphone Arbitrary Code Execution
  - WP-Stats SQL Injection
  - Helm Web Hosting Control Panel Cross-Site Scripting
  - Helmsman HomeFtp Denial of Service
  - Interspire TrackPoint NX Cross-Site Scripting
  - Microsoft Internet Explorer Denial of Service
  - **Microsoft Visual Studio Arbitrary Code Execution (Updated)**
  - **Microsoft Windows WMF Rendering Engine Arbitrary Code Execution (Updated)**
  - Mini-NUKE SQL Injection or Security Bypass
  - Mozilla Thunderbird Arbitrary Code Execution
  - Toshiba Bluetooth Information Disclosure
  - WehnTrust Privilege Elevation
- Unix/ Linux Operating Systems
  - CMU SNMP Format String
  - **ClamAV UPX File Handling (Updated)**
  - DCP Portal Multiple Input Validation
  - FreeBSD IEEE 802.11 Network Subsystem Remote Buffer Overflow
  - **GNU Mailman Attachment Scrubber UTF8 Filename Remote Denial of Service (Updated)**
  - GRSecurity Elevated Service Privileges
  - **Multiple Vendors Xpdf Buffer Overflows (Updated)**
  - **Multiple Vendors HylaFAX Authentication Bypass & Arbitrary Command Execution (Updated)**
  - **Multiple Vendors Sudo Python Environment Cleaning Security Bypass (Updated)**
  - **GTK+ GdkPixbuf XPM Image Rendering Library (Updated)**
  - Multiple Vendors Antiword Insecure Temporary File Creation
  - **Multiple Vendors KPdf & KWord Multiple Unspecified Buffer & Integer Overflow (Updated)**
  - **Multiple Vendors Linux Kernel routing_ioctl() Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel Multiple Vulnerabilities (Updated)**
  - **Multiple Vendors Linux Kernel 'Sysctl' Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel Denials of Service (Updated)**
  - **Multiple Vendors Linux Kernel PrintK Local Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel PTraced Denial of Service (Updated**
  - Multiple Vendors Linux Kernel ProcFS Kernel Memory Disclosure
  - **Multiple Vendors Network Block Device Server Buffer Overflow (Updated)**
  - Multiple Vendors Linux Kernel 'mq_open' System Call Denial of Service
  - **Multiple Vendors mod_auth_pgsql Apache Module Format String (Updated)**
  - **Multiple Vendors Fetchmail Remote Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel IPv6 FlowLable Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel SCSI ProcFS Denial of Service (Updated)**
  - Multiple Vendors GNU Mailman Remote Denial of Service
  - **Multiple Vendors Linux Kernel Information Disclosure (Updated)**
  - **Multiple Vendors Util-Linux UMount Remounting Filesystem Elevated Privileges**

Vulnerabilities

The tables below summarize vulnerabilities that have been reported by various open source organizations or presented in newsgroups and on web sites. **Items in bold designate updates that have been made to past entries.** Entries are grouped by the operating system on which the reported software operates, and vulnerabilities which affect both Windows and Unix/ Linux Operating Systems are included in the Multiple Operating Systems table. *Note*, entries in each table are not necessarily vulnerabilities *in* that operating system, but vulnerabilities in software which operate on some version of that operating system.

Entries may contain additional US-CERT sponsored information, including Common Vulnerabilities and Exposures (CVE) numbers, National Vulnerability Database (NVD) links, Common Vulnerability Scoring System (CVSS) values, Open Vulnerability and Assessment Language (OVAL) definitions, or links to US-CERT Vulnerability Notes. Metrics, values, and information included in the Cyber Security Bulletin which has been provided by other US-CERT sponsored programs, is prepared, managed, and contributed by those respective programs. CVSS values are managed and provided by the US-CERT/ NIST National Vulnerability Database. Links are also provided to patches and workarounds that have been provided by the product's vendor.

The Risk levels are defined below:

High - Vulnerabilities will be labeled "High" severity if they have a CVSS base score of 7.0-10.0.

Medium - Vulnerabilities will be labeled "Medium" severity if they have a base CVSS score of 4.0-6.9.

Low - Vulnerabilities will be labeled "Low" severity if they have a CVSS base score of 0.0-3.9.

Note that scores provided prior to 11/9/2005 are approximated from only partially available CVSS metric data. Such scores are marked as "Approximated" within NVD. In particular, the following CVSS metrics are only partially available for these vulnerabilities and NVD assumes certain values based on an approximation algorithm: AccessComplexity, Authentication, ConfImpact of 'partial', IntegImpact of 'partial', AvailImpact of 'partial', and the impact biases.

Windows Operating Systems Only

Vendor & Software Name	Description	Common Name	CVSS	Resources
AmbiCom Blue Neighbors Bluetooth 2.50 build 2500	A buffer overflow vulnerability has been reported in AmbiCom Blue Neighbors Bluetooth that could let remote malicious users to execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	AmbiCom Blue Neighbors Bluetooth Arbitrary Code Execution CVE-2006-0253	1.9	Security Focus, ID: 16258, January 16, 2006
America OnLine AOL Client Software 9.0, 8.0+, 8.0	A buffer overflow vulnerability has been reported in the 'You've Got Pictures' ActiveX control due to a runtime error, which could let a remote malicious user cause a Denial of Service	AOL You've Got Pictures ActiveX Control Remote Buffer Overflow CVE-2006-0316	Not available	Security Focus, ID: 16262, January 16, 2006 US-CERT VU#715730

	and potentially execute arbitrary code. AOL Currently we are not aware of any exploits for this vulnerability.			
ASPSurvey ASPSurvey 1.10	A vulnerability has been reported in ASPSurvey that could let remote malicious users perform SQL injection. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	ASPSurvey SQL Injection CVE-2006-0192	7	Secunia, Advisory: SA18422, January 12, 2006
BlogPHP BlogPHP 1.0	A vulnerability has been reported in BlogPHP that could let remote malicious users perform SQL injection. No workaround or patch available at time of publishing. There is no exploit code required.	BlogPHP SQL Injection CVE-2006-0318	7	Secunia, Advisory: SA18467, January 17, 2006
Check Point Software VPN-1 SecureClient 14.1 SP6 and prior	A vulnerability has been reported in VPN-1 SecureClient that could let local malicious users obtain elevated privileges. No workaround or patch available at time of publishing. There is no exploit code required.	Check Point VPN-1 SecureClient Privilege Elevation CVE-2006-0255	7	Security Focus, ID: 16290, January 17, 2006
Computer Associates Unicenter Remote Control 5.0, 6.0, 6.0SP1, German GA 6.0, French GA 6.0, English GA 6.0	A vulnerability has been reported in Unicenter Remote Control that could let remote malicious users cause a Denial of Service. No workaround or patch available at time of publishing.	Computer Associates Unicenter Remote Control Denial of Service CVE-2006-0306 CVE-2006-0307	2.3 (CVE-2006-0306) 2.3 (CVE-2006-0307)	Security Focus, ID: 16276, January 17, 2006

	There is no exploit code required; however, a Proof of Concept exploit has been published.			
DDSN Interactive CM3CMS	A vulnerability has been reported in CM3CMS that could let remote malicious users perform SQL injection. No workaround or patch available at time of publishing. There is no exploit code required.	CM3CMS SQL Injection CVE-2006-0221	7	Security Focus, ID: 16231, January 13, 2006
eStara Softphone 3.0.1.14, 3.0.1.46	A buffer overflow vulnerability has been reported in Softphone, SIP packet SDP data, that could let remote malicious users execute arbitrary code. No workaround or patch available at time of publishing. An exploit script, sip_overflow_exploit.c, has been published.	eStara Softphone Arbitrary Code Execution CVE-2006-0189	2.3	Security Tracker, Alert ID: 1015481, January 12, 2006
Gamerz WP-Stats 2.0	A vulnerability has been reported in WP-Stats that could let remote malicious users perform SQL injection. Gamerz There is no exploit code required.	WP-Stats SQL Injection CVE-2006-0238	7	Secunia, Advisory: SA18471, January 16, 2006
Helm Web Hosting Control Panel Helm Web Hosting Control Panel 3.2.8	A vulnerability has been reported in Helm Web Hosting Control Panel that could let remote malicious users conduct Cross-Site Scripting. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of	Helm Web Hosting Control Panel Cross-Site Scripting CVE-2006-0211	2.3	Secunia, Advisory: SA18492, January 16, 2006

	Concept exploit has been published.			
Helmsman HomeFTP 1.01	A vulnerability has been reported in Helmsman HomeFTP that could let remote malicious users cause a Denial of Service. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits, homeftp_dos.c and homeftp_v1.1_xpl.c, have been published.	Helmsman HomeFtp Denial of Service	Not available	Security Focus, ID: 16238, January 14, 2006
Interspire TrackPoint NX	A vulnerability has been reported in TrackPoint NX that could let remote malicious users conduct Cross-Site Scripting. Interspire There is no exploit code required; however, a Proof of Concept exploit has been published.	Interspire TrackPoint NX Cross-Site Scripting CVE-2006-0210	2.3	Security Focus, ID: 16214, January 12, 2006
Microsoft Internet Explorer	A vulnerability has been reported in Internet Explorer, IMG elements in XML parsing, that could let remote malicious users cause a Denial of Service. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Microsoft Internet Explorer Denial of Service	Not available	Security Focus, ID: 16240, January 16, 2006

Microsoft **Visual Studio 2005**	A vulnerability has been reported in Visual Studio that could let remote malicious users to execute arbitrary code. No workaround or patch available at time of publishing. **An exploit script, VSexploit.zip, has been published.**	Microsoft Visual Studio Arbitrary Code Execution CVE-2006-0187	**3.9**	Secunia, Advisory: SA18409, January 11, 2006 Security Focus, ID: 16225, January 13, 2006
Microsoft Windows Meta File (WMF) Graphics Rendering Engine	A vulnerability has been reported in Windows Meta File (WMF) Graphics Rendering Engine could let remote malicious users execute arbitrary code. Microsoft Avaya **Nortel** Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows WMF Rendering Engine Arbitrary Code Execution CVE-2005-4560	**7**	Microsoft, Security Advisory 912840, December 28, 2005 Vulnerability Note, VU#181038, December 27, 2005 Avaya, Number: ASA-2006-001, January 5, 2006 **Nortel, Bulletin 2006006572, January 16, 2006**
Mini-Nuke	A vulnerability has been reported in Mini-Nuke that could let remote malicious users to perform SQL injection or bypass security restrictions. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Mini-NUKE SQL Injection or Security Bypass CVE-2006-0199	Not available	Secunia, Advisory: SA18439, January 13, 2006
Mozilla Thunderbird 1.0.2, 1.0.6, and 1.0.7	A vulnerability has been reported in Thunderbird that could let remote malicious users execute	Mozilla Thunderbird Arbitrary Code Execution	3.9	Secunia, Advisory: SA15907, January 17, 2006

	arbitrary code. Mozilla Thunderbird 1.5 There is no exploit code required.	CVE-2006-0236		
Toshiba Bluetooth 4.00.23(T) & prior	An input validation vulnerability has been reported in Toshiba Bluetooth that could let remote malicious users to disclose information. No workaround or patch available at time of publishing. There is no exploit code required.	Toshiba Bluetooth Information Disclosure CVE-2006-0212	2.3	Security Tracker, Alert ID: 1015486, January 13, 2006
Wehnus WehnTrust	A vulnerability has been reported in WehnTrust that could let local malicious users obtain elevated privileges. No workaround or patch available at time of publishing. There is no exploit code required.	WehnTrust Privilege Elevation CVE-2006-0229	1.6	Security Focus, ID: 16268, January 16, 2006

[back to top

UNIX / Linux Operating Systems Only

Vendor & Software Name	Description	Common Name	CVSS	Resources
Carnegie Mellon University CMU SNMP 3.7, 3.6	A format string vulnerability has been reported in 'snmptrapd' when handling a SNMP trap request packet, which could let a malicious user cause a Denial of Service and potentially execute arbitrary code. The product is no longer being maintained. Currently we are not aware of any exploits for this vulnerability.	CMU SNMP Format String CVE-2006-0250	4.7	Secunia Advisory: SA18525, January 17, 2006

Clam Anti-Virus ClamAV 0.80 - 0.87.1, 0.75.1, 0.70, 0.68, 0.67, 0.65, 0.60, 0.51-0.54	A buffer overflow vulnerability has been reported when attempting to handle compressed UPX files due to an unspecified boundary error in "libclamav/upx.c, which could let a remote malicious user execute arbitrary code. ClamAV **SuSE** **Trustix** **Gentoo** **Mandriva** Currently we are not aware of any exploits for this vulnerability.	ClamAV UPX File Handling CVE-2006-0162	8	Secunia Advisory: SA18379, January 10, 2006 **US-CERT VU#385908** **SUSE Security Summary Report, SUSE-SR:2006:001, January 13, 2006** **Trustix Secure Linux Security Advisory, 2006-0002, January 13, 2006** **Gentoo Linux Security Advisory, GLSA 200601-07, January 13, 2006** **Mandriva Security Advisory, MDKSA-2006:016, January 16, 2006**
DCP-Portal DCP-Portal 6.1.1, 6.1, 6.0, 5.3-5.3.2	Multiple Cross-Site Scripting vulnerabilities have been reported in 'calendar.php' due to insufficient sanitization of the 'day' parameter and in 'search.php' due to insufficient sanitization of the input form, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	DCP Portal Multiple Input Validation CVE-2006-0220	2.3	Security Focus, Bugtraq ID: 16232, January 13, 2006
FreeBSD FreeBSD 6.0 -STABLE, 6.0 -RELEASE	A buffer overflow vulnerability has been reported in the 'net80211' module when handling corrupt IEEE 802.11 beacons or probe response frames when scanning for existing wireless networks, which could let a remote malicious user execute arbitrary code. Patches available	FreeBSD IEEE 802.11 Network Subsystem Remote Buffer Overflow CVE-2006-0226	10	FreeBSD Security Advisory, FreeBSD-SA-06:05.80211, January 18, 2006

	Currently we are not aware of any exploits for this vulnerability.			
GNU Mailman 2.1-2.1.5, 2.0-2.0.14	A remote Denial of Service vulnerability has been reported in 'Scrubber.py' due to a failure to handle exception conditions when Python fails to process an email file attachment that contains utf8 characters in its filename. Mandriva **SuSE** **Ubuntu** There is no exploit code required.	GNU Mailman Attachment Scrubber UTF8 Filename Remote Denial of Service CVE-2005-3573	5	Secunia Advisory: SA17511, November 14, 2005 Mandriva Linux Security Advisory, MDKSA-2005:222, December 2, 2005 **SUSE Security Summary Report, SUSE-SR:2006:001, January 13, 2006** **Ubuntu Security Notice, USN-242-1 January 16, 2006**
grsecurity grsecurity Kernel Patch 2.1.0-2.1.7, 2.0.2, 2.0.1	A vulnerability has been reported due to a failure to properly drop administrative roles, which could allow services to run with elevated privileges. Updates available Currently we are not aware of any exploits for this vulnerability.	GRSecurity Elevated Service Privileges CVE-2006-0228	7	Security Focus, Bugtraq ID: 16261, January 16, 2006
Multiple Vendors Xpdf 3.0 pl2 & pl3, 3.0 1, 3.00, 2.0-2.03, 1.0 0, 1.0 0a, 0.90-0.93; RedHat Fedora Core4, Core3, Enterprise Linux WS 4, WS 3, WS 2.1 IA64, WS 2.1, ES 4, ES 3, ES 2.1 IA64, 2.1, Enterprise Linux AS 4, AS 3, 2.1 IA64, 2.1, Desktop 4.0, 3.0, Advanced Workstation for the Itanium Processor 2.1 IA64, 2.1; teTeX 2.0.1, 2.0; Poppler poppler 0.4.2; KDE kpdf 0.5, KOffice 1.4.2 ; PDFTOHTML DFTOHTML 0.36	Multiple vulnerabilities have been reported: a heap-based buffer overflow vulnerability was reported in the 'DCTStream::read BaselineSOF()' function in 'xpdf/Stream.cc' when copying data from a PDF file, which could let a remote malicious user potentially execute arbitrary code; a buffer overflow vulnerability was reported in the 'DCTStream::read ProgressiveSOF()' function in 'xpdf/Stream.cc' when copying data from a PDF file, which could let a remote malicious user potentially execute arbitrary code; a buffer	Xpdf Buffer Overflows CVE-2005-3191 CVE-2005-3192 CVE-2005-3193	4.8 (CVE-2005-3191) 7 (CVE-2005-3192) 4.8 (CVE-2005-3193)	iDefense Security Advisory, December 5, 2005 Fedora Update Notifications, FEDORA-2005-1121 & 1122, December 6, 2005 RedHat Security Advisory, RHSA-2005:840-5, December 6, 2005 KDE Security Advisory, advisory-20051207-1, December 7, 2005 SUSE Security Summary Report, SUSE-SR:2005:029, December 9, 2005 Ubuntu Security Notice, USN-227-1, December 12, 2005

	overflow vulnerability was reported in the 'StreamPredictor:: StreamPredictor()' function in 'xpdf/Stream.cc' when using the 'numComps' value to calculate the memory size, which could let a remote malicious user potentially execute arbitrary code; and a vulnerability was reported in the 'JPXStream: :readCodestream()' function in 'xpdf/JPXStream.cc' when using the 'nXTiles' and 'nYTiles' values from a PDF file to copy data from the file into allocated memory, which could let a remote malicious user potentially execute arbitrary code. Patches available Fedora RedHat KDE SUSE Ubuntu Gentoo RedHat RedHat RedHat Mandriva Debian **Debian** **Debian** **Fedora** **SuSE** Currently we are not aware of any exploits for these vulnerabilities.			Gentoo Linux Security Advisory, GLSA 200512-08, December 16, 2005 RedHat Security Advisories, RHSA-2005:868-4, RHSA-2005:867-5 & RHSA-2005:878-4, December 20, 2005 Mandriva Linux Security Advisories MDKSA-2006:003-003-006, January 6, 2006 Debian Security Advisory, DSA-936-1, January 11, 2006 **Debian Security Advisory, DSA-937-1, January 12, 2006** **Debian Security Advisory, DSA 938-1, January 12, 2006** **Fedora Update Notifications, FEDORA-2005-028 & 029, January 12, 2006** **SUSE Security Summary Report, SUSE-SR:2006:001, January 13, 2006**
Multiple Vendors Hylafax 4.2-4.2.3;	Several vulnerabilities have been reported: a vulnerability was reported	HylaFAX Authentication	7 (CVE-2005-3538)	Secunia Advisory: SA18314, January 6, 2006

Gentoo Linux	in 'hfaxd' when compiled with PAM support disabled, which could let a remote malicious user obtain unauthorized access; a vulnerability was reported due to insufficient sanitization of the 'notify' script, which could let a remote malicious user execute arbitrary commands; and a vulnerability was reported in the 'faxrcvd' script due to insufficient sanitization, which could let a remote malicious user execute arbitrary commands. Hylafax Gentoo **Mandriva** There is no exploit code required; however, Proof of Concept exploits have been published.	Bypass & Arbitrary Command Execution CVE-2005-3538 CVE-2005-3539	8 (CVE-2005-3539)	Gentoo Linux Security Advisory GLSA 200601-03, January 6, 2006 **Mandriva Security Advisory, MDKSA-2006:015, January 16, 2006**
Multiple Vendors Ubuntu Linux 5.10 powerpc, i386, amd64, 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Todd Miller Sudo 1.6-1.6.8, 1.5.6-1.5.9	A vulnerability has been reported in the 'PYTHONINSPECT' variable, which could let a malicious user bypass security restrictions and obtain elevated privileges. Todd Miller Sudo AppleWebSharing Update Conectiva Debian EnGarde Fedora FreeBSD GratiSoft Sudo Mandriva OpenPKG OpenBSD RedHat Slackware	Sudo Python Environment Cleaning Security Bypass CVE-2006-0151	7	Security Focus, Bugtraq ID: 16184, January 9, 2006 **Security Focus, Bugtraq ID: 16184, January 12, 2006**

SuSE

Trustix

TurboLinux

Ubuntu

Wirex

An exploit script, sudo_local_python_exploit.txt, has been published.

Multiple Vendors Ubuntu Linux 5.10 powerpc, i386, amd64, 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; TouchTunes Rhapsody, TouchTunes Maestro; SuSE UnitedLinux 1.0, Novell Linux Desktop 9.0, Linux Professional 10.0 OSS, 10.0, 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, 9.0 x86_64, 9.0, Linux Personal 10.0 OSS, 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, 9.0 x86_64, 9.0, Linux Enterprise Server 9, 8, Linux Desktop 1.0; RedHat Fedora Core4, Core3, Enterprise Linux WS 4, WS 3, WS 2.1 IA64, WS 2.1, ES 4, ES 3, 2.1 IA64, 2.1, AS 4, AS 3, AS 2.1 IA64, 2.1, Desktop 4.0, 3.0, Advanced Workstation for the Itanium Processor 2.1 IA64, 2.1; GTK+ 2.8.6, 2.6.4, 2.4.14, 2.4.13, 2.4.10, 2.4.9, 2.4.1, 2.2.4, 2.2.3; GNOME GdkPixbuf 0.22; Gentoo Linux ; Ardour 0.99	Multiple vulnerabilities have been reported: an integer overflow vulnerability was reported in '/gtk+/gdk-pixbuf/io-xpm.c' due to the insufficient validation of the 'n_col' value before using to allocate memory, which could let a remote malicious user execute arbitrary code; a remote Denial of Service vulnerability was reported in '/gtk+/gdk-pixbuf/io-xpm.c' when processing an XPM file that contains a large number of colors; and an integer overflow vulnerability was reported in '/gtk+/gdk-pixbuf/io-xpm.c' when performing calculations using the height, width, and colors of a XPM file, which could let a remote malicious user execute arbitrary code or cause a Denial of Service. Updates available Fedora RedHat Gentoo SuSE Ubuntu Mandriva Trustix Avaya Debian SG Debian **SCO** Currently we are not aware of any exploits for these vulnerabilities.	GTK+ GdkPixbuf XPM Image Rendering Library CVE-2005-2975 CVE-2005-2976 CVE-2005-3186	5 (CVE-2005-2975) 9 (CVE-2005-2976) 8.5 (CVE-2005-3186)	Fedora Update Notifications FEDORA-2005-1085 & 1086, November 15, 2005 RedHat Security Advisory, RHSA-2005:810-9, November 15, 2005 Gentoo Linux Security Advisory GLSA 200511-14, November 16, 2005 SUSE Security Announcement, SUSE-SA:2005:065, November 16, 2005 Ubuntu Security Notice, USN-216-1, November 16, 2005 Mandriva Linux Security Advisory, MDKSA-2005:214, November 18, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0066, November 22, 2005 Avaya Security Advisory, ASA-2005-229, November 21, 2005 Debian Security Advisory, DSA 911-1, November 29, 2005 SGI Security Advisory, 20051101-01-U, November 29, 2005 Debian Security Advisory DSA 913-1, December 1, 2005 **SCO Security Advisory, SCOSA-2006.8, January 13, 2006**
Multiple Vendors Debian Linux 3., sparc,	A vulnerability has been reported in the 'kantiword'	Antiword Insecure	4.9	Debian Security Advisory, DSA-945-1, January 17,

s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha, 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; Antiword 0.35, 0.32	and 'gantiword' scripts due to the insecure creation of temporary files, which could let a malicious user obtain elevated privileges. Debian There is no exploit code required.	Temporary File Creation CVE-2005-3126		2006
Multiple Vendors KDE kword 1.4.2, kpdf 3.4.3, 3.2, KOffice 1.4-1.4.2, kdegraphics 3.4.3, 3.2; Gentoo Linux	Multiple buffer and integer overflows have been reported, which could let a remote malicious user execute arbitrary code. Gentoo Ubuntu Fedora Mandriva Ubuntu Debian Debian **SuSE** **RedHat** **RedHat** **Fedora** **Debian** **Trustix** **Mandriva** Currently we are not aware of any exploits for this vulnerability.	KPdf & KWord Multiple Unspecified Buffer & Integer Overflow CVE-2005-3624 CVE-2005-3625 CVE-2005-3626 CVE-2005-3627	Not available	Gentoo Linux Security Advisory GLSA 200601-02, January 5, 2006 Ubuntu Security Notice, USN-236-1, January 05, 2006 Fedora Update Notifications, FEDORA-2005-000, January 5, 2006 Mandriva Linux Security Advisories MDKSA-2006:003-003-006 & 008, January 6 & 7, 2006 Ubuntu Security Notice, USN-236-2, January 09, 2006 Debian Security Advisory DSA 931-1, January 9, 2006 Debian Security Advisory, DSA-936-1, January 11, 2006 **SUSE Security Announcement, SUSE-SA:2006:001, January 11, 2006** **RedHat Security Advisories, RHSA-2006:0163-2 & RHSA-2006:0177-5, January 11, 2006** **Fedora Update Notifications, FEDORA-2005-028 & 029, January 12, 2006** **Debian Security Advisories, DSA 937-1, 938-1, & 940-1, January 12 & 13, 2006** **Trustix Secure Linux**

				Security Advisory, 2006-0002, January 13, 2006 **Mandriva Linux Security Advisory, MDKSA-2006:012, January 13, 2006**
Multiple Vendors Linux kernel 2.6-2.6.13.1	A Denial of Service vulnerability has been reported due to an omitted call to the 'sockfd_put()' function in the 32-bit compatible 'routing_ioctl()' function. Linux Kernel Ubuntu Mandriva SUSE Conectiva **RedHat** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel routing_ioctl() Denial of Service CVE-2005-3044	2.3	Security Tracker Alert ID: 1014944, September 21, 2005 Ubuntu Security Notice, USN-187-1, September 25, 2005 Mandriva Linux Security Advisories, MDKSA-2005:218, 219, 220, November 30, 2005 SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005 SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005 Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006 **RedHat Security Advisory, RHSA-2006:0101-9, January 17, 2006**
Multiple Vendors Linux kernel 2.6-2.6.14	Multiple vulnerabilities have been reported: a Denial of Service vulnerability was reported in 'mm/mempolicy.c' when handling the policy system call; a remote Denial of Service vulnerability was reported in 'net/ipv4/fib_ frontend.c' when validating the header and payload of fib_lookup netlink messages; an off-by-one buffer overflow vulnerability was reported in 'kernel/sysctl.c,' which could let a malicious user cause a Denial of Service and potentially execute arbitrary code; and a buffer overflow	Linux Kernel Multiple Vulnerabilities CVE-2005-3358	3.5	Secunia Advisory: SA18216, January 4, 200 **RedHat Security Advisory, RHSA-2006:0101-9, January 17, 2006**

	vulnerability was reported in the DVB (Digital Video Broadcasting) driver subsystem, which could let a malicious user cause a Denial of Service or potentially execute arbitrary code. Upgrades available **RedHat** An exploit script has been published.			
Multiple Vendors Linux kernel 2.6-2.6.14	A Denial of Service vulnerability has been in 'sysctl.c' due to an error when handling the un-registration of interfaces in '/proc/sys/net/ipv4/conf/.' Upgrades available Ubuntu **RedHat** There is no exploit code required.	Linux Kernel 'Sysctl' Denial of Service CVE-2005-2709	6	Secunia Advisory: SA17504, November 9, 2005 Ubuntu Security Notice, USN-219-1, November 22, 2005 **RedHat Security Advisory, RHSA-2006:0101-9, January 17, 2006**
Multiple Vendors Linux Kernel 2.6-2.6.14	Multiple vulnerabilities have been reported: a Denial of Service vulnerability was reported in the 'sys_set_mempolicy' function when a malicious user submits a negative first argument; a Denial of Service vulnerability was reported when threads are sharing memory mapping via 'CLONE_VM'; a Denial of Service vulnerability was reported in 'fs/exec.c' when one thread is tracing another thread that shares the same memory map; a Denial of Service vulnerability was reported in 'mm/ioremap.c' when performing a lookup of a non-existent page; a Denial of Service vulnerability was reported in the HFS and HFS+ (hfsplus) modules; and a remote Denial of Service vulnerability was reported	Multiple Vendors Linux Kernel Denials of Service CVE-2005-3053 CVE-2005-3106 CVE-2005-3107 CVE-2005-3108 CVE-2005-3109 CVE-2005-3110	2.3 (CVE-2005-3053) 2.3 (CVE-2005-3106) 2.3 (CVE-2005-3107) 2.3 (CVE-2005-3108) 2.3 (CVE-2005-3109) 3.3 (CVE-2005-3110)	Ubuntu Security Notice, USN-199-1, October 10, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0057, October 14, 2005 RedHat Security Advisory, RHSA-2005:808-14, October 27, 2005 Mandriva Linux Security Advisories, MDKSA-2005: 219 & 220, November 30, 2005 SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005 Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006 **RedHat Security Advisory, RHSA-2006:0101-9, January 17, 2006**

	due to a race condition in 'ebtables.c' when running on a SMP system that is operating under a heavy load. Ubuntu Trustix RedHat Mandriva SUSE Conectiva **RedHat** Currently we are not aware of any exploits for these vulnerabilities.			
Multiple Vendors Linux kernel 2.6-2.6.15	A Denial of Service vulnerability has been reported in the 'time_out_leases()' function because 'printk()' can consume large amounts of kernel log space. Patches available Trustix **RedHat** An exploit script has been published.	Linux Kernel PrintK Local Denial of Service CVE-2005-3857	3.5	Security Focus, Bugtraq ID: 15627, November 29, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0070, December 9, 2005 **RedHat Security Advisory, RHSA-2006:0101-9, January 17, 2006**
Multiple Vendors Linux kernel 2.6-2.6.15; SuSE Linux Professional 10.0 OSS, Linux Personal 10.0 OSS; RedHat Fedora Core4	A Denial of Service vulnerability has been reported because processes are improperly auto-reaped when they are being ptraced. Patches available Fedora Trustix SUSE **RedHat** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel PTraced Denial of Service CVE-2005-3784	3.5	Security Focus, Bugtraq ID: 15625, November 29, 2005 Fedora Update Notification, FEDORA-2005-1104, November 28, 2005 SuSE Security Announcement, SUSE-SA:2005:067, December 6, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0070, December 9, 2005 SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005 **RedHat Security**

				Advisory, RHSA-2006:0101-9, January 17, 2006
Multiple Vendors Linux kernel prior to 2.6.15	A memory disclosure vulnerability has been reported in the 'ProcFS' kernel, which could let a malicious user obtain sensitive information. Update available Fedora RedHat Ubuntu Currently we are not aware of any exploits for this vulnerability.	Linux Kernel ProcFS Kernel Memory Disclosure CVE-2005-4605	1.6	Security Focus, Bugtraq ID: 16284, January 17, 2006 RedHat Security Advisory, RHSA-2006:0101-9, January 17, 2006 Ubuntu Security Notice, USN-244-1, January 18, 2006
Multiple Vendors Network Block Device NBD 2.8-2.8.2, 2.7.5; Gentoo Linux; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha, 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha	A buffer overflow vulnerability has been reported in the 'nbd-server' when handling specially crafted requests, which could let a remote malicious user execute arbitrary code. Upgrades available Debian Gentoo Ubuntu **SuSE** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Network Block Device Server Buffer Overflow CVE-2005-3534	7	Security Focus, Bugtraq ID: 16029, December 21, 2005 Debian Security Advisory, DSA 924-1, December 21, 2005 Gentoo Linux Security Advisory, GLSA 200512-14, December 23, 2006 Ubuntu Security Notice, USN-237-1, January 06, 2006 **SUSE Security Summary Report, SUSE-SR:2006:001, January 13, 2006**
Multiple Vendors RedHat Enterprise Linux WS 4, ES 4, AS 4, Desktop 4.0; Linux kernel 2.6.9	A Denial of Service vulnerability has been reported in the 'mq_open' system call. RedHat Ubuntu Currently we are not aware of any exploits for this vulnerability.	Linux Kernel 'mq_open' System Call Denial of Service CVE-2005-3356	Not available	Security Focus, Bugtraq ID: 16283, January 17, 2006 RedHat Security Advisory, RHSA-2006:0101-9, January 17, 2006 Ubuntu Security Notice, USN-244-1, January 18, 2006
Multiple Vendors RedHat Enterprise Linux WS 4, WS 3, ES 4, ES 3, AS 4, AS 3, Desktop 4.0, 3.0;	A format string vulnerability has been reported in 'mod_auth_pgsql' when logging information, which could let a remote	Multiple Vendors mod_auth_pgsql Apache Module Format String	Not available	RedHat Security Advisory, RHSA-2006:0164-7, January 5, 2006 Fedora Update Notifications,

mod_auth_pgsql 2.0.1	malicious user execute arbitrary code. mod_auth_pgsql RedHat Fedora Mandriva Ubuntu **Debian** **Gentoo** **Trustix** Currently we are not aware of any exploits for this vulnerability.	CVE-2005-3656		FEDORA-2005-014 & 015, January 6, 2005 Mandriva Linux Security Advisory, MDKSA-2006:009, January 7, 2006 Ubuntu Security Notice, USN-239-1, January 09, 2006 **Debian Security Advisory, DSA 935-1, January 10, 2006** **Gentoo Linux Security Advisory, GLSA 200601-05, January 10, 2006** **Trustix Secure Linux Security Advisory, 2006-0002, January 13, 2006**
Multiple Vendors RedHat Fedora Core4, Core3; Eric Raymond Fetchmail 6.3.0, 6.2.5 .4, 6.2.5 .2, 6.2.5.1, 6.2.5	A remote Denial of Service vulnerability has been reported when Fetchmail is configured in 'multidrop' mode due to a failure to handle unexpected input. Upgrades available Fedora Mandriva Ubuntu **Debian** **Trustix** There is no exploit code required.	Fetchmail Remote Denial of Service CVE-2005-4348	3.3	Security Focus, Bugtraq ID: 15987, December 20, 2005 Fedora Update Notifications FEDORA-2005-1186 & 1187, December 20, 2005 Mandriva Linux Security Advisory MDKSA-2005:236, December 23, 2005 Ubuntu Security Notice, USN-233-1 January 02, 2006 **Debian Security Advisory, DSA 939-1, January 13, 2006** **Trustix Secure Linux Security Advisory, 2006-0002, January 13, 2006**

Multiple Vendors SuSE Linux Professional 10.0 OSS, 10.0, Personal 10.0 OSS; Linux kernel 2.6-2.6.13, Linux kernel 2.4-2.4.32	A Denial of Service vulnerability has been reported in FlowLable. Upgrades available SUSE **RedHat** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel IPv6 FlowLable Denial of Service CVE-2005-3806	5.3	Security Focus, Bugtraq ID: 15729, December 6, 2005 SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005 SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005 **RedHat Security Advisory, RHSA-2006:0101-9, January 17, 2006**
Multiple Vendors Ubuntu Linux 5.0 4, i386, amd64, 4.1 ppc, ia64, ia32; Linux kernel 2.6-2.6.13	A Denial of Service vulnerability has been reported in the '/proc/scsi/sg/devices' file due to a memory leak. Ubuntu Mandriva SUSE Conectiva **RedHat** A Proof of Concept exploit has been published.	Linux Kernel SCSI ProcFS Denial of Service CVE-2005-2800	2.3	Security Focus, Bugtraq ID: 14790, September 9, 2005 Ubuntu Security Notice, USN-178-1, September 09, 2005 Mandriva Linux Security Advisories, MDKSA-2005:218, 219, & 220, November 30, 2005 SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005 Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006 **RedHat Security Advisory, RHSA-2006:0101-9, January 17, 2006**
Multiple Vendors Ubuntu Linux 5.10 powerpc, i386, amd64, 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; MandrakeSoft Linux Mandrake 2006.0 x86_64, 2006.0, 10.2 x86_64, 10.2, 10.1 x86_64, 10.1, Corporate Server 3.0 x86_64, 3.0; GNU Mailman 2.1-2.1.5, 2.0-2.0.14	A remote Denial of Service vulnerability has been reported in the email date parsing functionality due to an error in the handling of dates. Mandriva Ubuntu There is no exploit code required.	GNU Mailman Remote Denial of Service CVE-2005-4153	3.3	Security Focus, Bugtraq ID: 16248, January 16, 2006 Ubuntu Security Notice, USN-242-1 January 16, 2006

Multiple Vendors Ubuntu Linux 5.10 powerpc, i386, amd64; Linux kernel 2.6-2.6.12 .3	An information disclosure vulnerability has been reported in 'SYS_GET_THREAD _AREA,' which could let a malicious user obtain sensitive information. Kernel versions 2.6.12.4 and 2.6.13 are not affected by this issue. Ubuntu Mandriva Debian Conectiva **RedHat** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Information Disclosure CVE-2005-3276	2.3	Ubuntu Security Notice, USN-219-1, November 22, 2005 Mandriva Linux Security Advisories, MDKSA-2005:218, 219 & 220, November 30, 2005 Debian Security Advisory, DSA 922-1, December 14, 2005 Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006 **RedHat Security Advisory, RHSA-2006:0101-9, January 17, 2006**
Multiple Vendors util-linux 2.8-2.13; Andries Brouwer util-linux 2.11 d, f, h, i, k, l, n, u, 2.10 s	A vulnerability has been reported because mounted filesystem options are improperly cleared due to a design flaw, which could let a remote malicious user obtain elevated privileges. Updates available Slackware Trustix Ubuntu Gentoo Mandriva Debian SUSE Conectiva Sun SGI FedoraLegacy **Avaya** There is no exploit code required.	Util-Linux UMount Remounting Filesystem Elevated Privileges CVE-2005-2876	7	Security Focus, Bugtraq ID: 14816, September 12, 2005 Slackware Security Advisory, SSA:2005-255-02, September 13, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0049, September 16, 2005 Ubuntu Security Notice, USN-184-1, September 19, 2005 Gentoo Linux Security Advisory, GLSA 200509-15, September 20, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:167, September 20, 2005 Debian Security Advisory, DSA 823-1, September 29, 2005 SUSE Security Summary Report, SUSE-SR:2005:021, September 30, 2005 Conectiva Linux Announcement,

				CLSA-2005:1022, October 6, 2005 Sun(sm) Alert Notification Sun Alert ID: 101960, October 10, 2005 SGI Security Advisor, 20051003-01-U, October 26, 2005 Fedora Legacy Update Advisory, FLSA:168326, December 17, 2005 **Avaya Security Advisory, ASA-2006-014, January 16, 2006**
Multiple Vendors Webmin 0.88 -1.230, 0.85, 0.76-0.80, 0.51, 0.42, 0.41, 0.31, 0.22, 0.21, 0.8.5 Red Hat, 0.8.4, 0.8.3, 0.1-0.7; Usermin 1.160, 1.150, 1.140, 1.130, 1.120, 1.110, 1.0, 0.9-0.99, 0.4-0.8; Larry Wall Perl 5.8.3-5.8.7, 5.8.1, 5.8 .0-88.3, 5.8, 5.6.1, 5.6, 5.0 05_003, 5.0 05, 5.0 04_05, 5.0 04_04, 5.0 04, 5.0 03	A format string vulnerability has been reported in 'Perl_sv_ vcatpvfnl' due to a failure to properly handle format specifiers in formatted printing functions, which could let a remote malicious user cause a Denial of Service. Webmin Fedora OpenPKG Mandriva Ubuntu Gentoo Gentoo Mandriva SUSE Trustix Ubuntu Fedora RedHat OpenBSD OpenBSD **Debian** An exploit has been published.	Perl 'miniserv.pl' script Format String CVE-2005-3912 CVE-2005-3962	9.3 (CVE-2005-3212) 6 (CVE-2005-3962)	Security Focus, Bugtraq ID: 15629, November 29, 2005 Fedora Update Notifications, FEDORA-2005-1113, 1116, & 1117, December 1 & 2, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.025, December 3, 2005 Mandriva Linux Security Advisory, MDKSA-2005:223, December 2, 2005 Ubuntu Security Notice, USN-222-1 December 02, 2005, December 2, 2005 Gentoo Linux Security Advisory, GLSA 200512-01 & 200512-02, December 7, 2005 US-CERT VU#948385 Mandriva Linux Security Advisory, MDKSA-2005:225, December 8, 2005 SUSE Security Summary Report, SUSE-SR:2005:029, December 9, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0070, December 9, 2005

				Ubuntu Security Notice, USN-222-2, December 12, 2005 Fedora Update Notifications, FEDORA-2005-1144 & 1145, December 14, 2005 SUSE Security Summary Report, SUSE-SR:2005:030, December 16, 2005 RedHat Security Advisory, RHSA-2005:880-8, December 20, 2005 Security Focus, Bugtraq ID: 15629, January 4, 2006 **Debian Security Advisory, DSA-943-1, January 16, 2006**
RedKernel Softwares Referrer Tracker 1.1 .0-3	A Cross-Site Scripting vulnerability has been reported in 'Rkrt_stats.PHP' due to insufficient sanitization before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	RedKernel Referrer Tracker Cross-Site Scripting CVE-2006-0317	2.3	Secunia Advisory: SA18473, January 16, 2006
Sun Microsystems, Inc. Solaris 10.0 _x86, 10.0	A Denial of Service vulnerability has been reported when the find(1) command is used to perform a search on the '/proc' filesystem due to an unspecified error. Sun There is no exploit code required.	Sun Solaris Find Denial of Service CVE-2006-0191	2.3	Sun(sm) Alert Notification Sun Alert ID: 102108, January 11, 2006

Sun Microsystems, Inc. Solaris 10.0 _x86, 10.0, 9.0 _x86, 9.0, 8.0 _x86, 8.0	Several vulnerabilities have been reported in 'lpsched(1M)' which could let a malicious user modify system/user information or cause a Denial or Service. Sun Currently we are not aware of any exploits for these vulnerabilities.	Sun Solaris 'LPSCHED' Vulnerabilities CVE-2006-0227	3.3	Sun(sm) Alert Notification Sun Alert ID: 102033, January 13, 2006
Sun Microsystems, Inc. Solaris 10.0, 9.0 _x86, 10_x86	A vulnerability was reported in the mm(5) driver, which could let a malicious user obtain root privileges or cause a Denial of Service. Sun Currently we are not aware of any exploits for this vulnerability.	Solaris x86 mm Driver Root Access CVE-2006-0190	7	Sun(sm) Alert Notification Sun Alert ID: 102066, January 11, 2006
SuSE Open-Enterprise-Server 9.0	A heap overflow vulnerability has been reported in the Novell Remote Manager (novell-nrm) due to improper handling of HTTP POST requests that contain a negative Content-Length parameter, which could let a remote malicious user arbitrary code. SuSE Currently we are not aware of any exploits for this vulnerability.	SuSE Open Enterprise Server Novell Remote Heap Overflow CVE-2005-3655	7	SUSE Security Announcement, SUSE-SA:2006:002, January 13, 2006
Todd Miller Sudo prior to 1.6.8p12	A vulnerability has been reported due to an error when handling the 'PERLLIB,' 'PERL5LIB,' and 'PERL5OPT' environment variables when tainting is ignored, which could let a malicious user bypass security restrictions and include arbitrary library files. Sudo Mandriva Ubuntu	Todd Miller Sudo Security Bypass CVE-2005-4158	4.9	Security Focus, Bugtraq ID: 15394, November 11, 2005 Mandriva Linux Security Advisory, MDKSA-2005:234, December 20, 2005 Ubuntu Security Notice, USN-235-1, January 05, 2006 **Trustix Secure Linux Security Advisory, 2006-0002, January 13, 2006**

	Trustix There is no exploit code required; however, a Proof of Concept exploit script has been published.			
Widexl Download Tracker 1.0.6	A Cross-Site Scripting vulnerability has been reported in 'Down.PL' due to insufficient sanitization of the 'ID' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	Widexl Download Tracker Cross-Site Scripting CVE-2006-0246	2.3	Security Focus, Bugtraq ID: 16265, January 16, 2006
xloadimage xloadimage 4.1	A buffer overflow vulnerability has been reported when handling the title of a NIFF image when performing zoom, reduce, or rotate functions, which could let a remote malicious user execute arbitrary code. Debian Debian RedHat Mandriva SUSE SGI Gentoo SCO **Avaya** Currently we are not aware of any exploits for this vulnerability.	Xloadimage NIFF Image Buffer Overflow CVE-2005-3178	3.9	Debian Security Advisories, DSA 858-1 & 859-1, October 10, 2005 RedHat Security Advisory, RHSA-2005:802-4, October 18, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:191, October 21, 2005 SUSE Security Summary Report, SUSE-SR:2005:024, October 21, 2005 SGI Security Advisory, 20051003-01-U, October 26, 2005 Gentoo Linux Security Advisory, GLSA 200510-26, October 31, 2005 SCO Security Advisory, SCOSA-2005.56, December 14, 2005 **Avaya Security Advisory, ASA-2006-013, January 16, 2006**

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Description	Common Name	CVSS	Resources
Advantage Century Telecommunication Corporation ACT WLAN Phone P202S	Multiple vulnerabilities have been reported: a vulnerability was reported on port 17185/udp because connections are allowed from the VxWorks WDB remote debugger, which could let a remote malicious user obtain sensitive information; a vulnerability was reported on port 7/tcp because connections to the echo service are allowed, which could lead to a Denial of Service; and a vulnerability was reported on port 513/tcp because connections to the rlogin service are allowed, which could let a remote malicious user obtain unauthorized access. No workaround or patch available at time of publishing. There is no exploit code required.	ACT P202S VOIP WIFI Phones Multiple Remote Vulnerabilities	Not available	Secunia Advisory: SA18514, January 17, 2006
Albatross Albatross 1.20	A vulnerability has been reported in 'context.py' due to an error when validating certain user-supplied data, which could let a remote malicious user execute arbitrary commands.	Albatross Arbitrary Command Execution CVE-2006-0044	7	Debian Security Advisory, DSA-942-1, January 16, 2006

	Update available Debian Currently we are not aware of any exploits for this vulnerability.			
AlstraSoft Template Seller Pro	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of 'fullview.php' before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	AlstraSoft Template Seller Pro Cross-Site Scripting CVE-2006-0222	2.3	Security Focus, Bugtraq ID: 16233, January 13, 2006
aoblogger aoblogger 2.3	Multiple input validation vulnerabilities have been reported: a vulnerability was when posting a comment via the 'url' bbcode tag due to insufficient verification, which could let a remote malicious user execute arbitrary script code; an SQL injection vulnerability was reported in 'login.php' due to insufficient sanitization of the 'username' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary	AOblogger Multiple Input Validation CVE-2006-0310 CVE-2006-0311 CVE-2006-0312	2.3 (CVE-2006-0310) 7 (CVE-2006-0311) 2.3 (CVE-2006-0312)	Secunia Advisory: SA16889, January 18, 2006

	SQL code; and a vulnerability was reported in 'create.php' when the 'uza' parameter is set to '1' due to an error in the authorization handling, which could let a remote malicious user obtain unauthorized access. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.			
Apache Software Foundation Geronimo 1.0	Multiple input validation vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user compromise the application, or obtain/modify information. Updates available There is no exploit code required; however, Proof of Concept exploits have been published.	Apache Geronimo Multiple Input Validation CVE-2006-0254	2.3	Security Focus, Bugtraq ID: 16260, January 16, 2006
Apache Software Foundation Apache prior to 1.3.35-dev, 2.0.56-dev	A Cross-Site Scripting vulnerability has been reported in the 'Referer' directive in 'mod_imap' due to insufficient sanitization before returning to the user, which could let a remote	Apache mod_imap Cross-Site Scripting CVE-2005-3352	2.3	Security Tracker Alert ID: 1015344, December 13, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.029, December 14, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0074,

	malicious user execute arbitrary HTML and script code. The vulnerability has been fixed in version 1.3.35-dev, and 2.0.56-dev. OpenPKG Trustix Mandriva **Ubuntu** **RedHat** There is no exploit code required.			December 23, 2005 Mandriva Linux Security Advisory, MDKSA-2006:007, January 6, 2006 **Ubuntu Security Notice, USN-241-1, January 12, 2006** **RedHat Security Advisory, RHSA-2006:0158-4, January 17, 2006**
BEA Systems, Inc. WebLogic Server & Express 6.1, 7.0, and 8.1, on all platforms	An information disclosure vulnerability was reported due to improper disclosure of configuration information, which could let a remote malicious user obtain sensitive information. workaround There is no exploit code required.	BEA WebLogic Server & WebLogic Express MBean Remote Information Disclosure CVE-2003-1290	Not available	BEA Security Advisory: BEA03-43.00, January 12, 2006
Benders Calendar Benders Calendar 1.0	SQL injection vulnerabilities have been reported in 'index.php' due to insufficient sanitization of certain parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof	Benders Calendar Multiple SQL Injection CVE-2006-0252	7	Security Tracker Alert ID: 1015491, January 16, 2006

	of Concept exploit has been published.			
Bit 5 Blog Bit 5 Blog 8.1	Several vulnerabilities have been reported: an SQL injection vulnerability was reported in 'processlogin.php' due to insufficient sanitization of the 'username' and 'password' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability was reported in 'addcomment.php' due to insufficient sanitization of the 'comment' parameter, which could let a remote malicious user execute arbitrary script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Bit 5 Blog Script Insertion & SQL Injection CVE-2006-0320	7	Secunia Advisory: SA18464, January 16, 2006
Cisco Systems Aironet 350 IOS, 1400, 1300, 1240AG, 1230AG, 1200, 1130AG, 1100	A remote Denial of Service vulnerability has been reported when handling an excessive number of ARP requests. Cisco There is no exploit code required.	Cisco Aironet Wireless Access Point ARP Remote Denial of Service	Not available	Cisco Security Advisory, cisco-sa-20060112, January 12, 2006
Cisco Systems CallManager 3.2 & prior, 3.3, versions earlier than	Multiple remote Denial of Service vulnerabilities have been reported due to a	Cisco CallManager Multiple Remote Denial of Service	Not available	Cisco Security Advisory, cisco-sa-20060118-ccmdos, January 18, 2006

3.3(5)SR1a, 4.0, versions earlier than 4.0(2a)SR2c, 4.1, versions earlier than 4.1(3)SR2	failure to manage TCP connections and Windows messages aggressively. Patches & workarounds There is no exploit code required.			
Cisco Systems Cisco Call Manager 4.1 (3)SR1, 4.1 (3)ES07, 4.1 (2)ES33, 4.0 (2a)SR2b, 4.0 (2a)ES40, 4.0, 3.3 (5), 3.3 (4)ES25, 3.3 (3)ES61, 3.3 (3), 3.3, 3.2, 3.1 (3a), 3.1 (2), 3.1, 3.0, 2.0, 1.0	A vulnerability has been reported in the 'CCMAdmin' web interface when Multi Level Administration is enabled due to insufficient access controls, which could let a remote malicious user obtain elevated privileges. Patches & workarounds There is no exploit code required.	Cisco CallManager CCMAdmin Remote Elevated Privileges	Not available	Cisco Security Advisory, cisco-sa-20060118-ccmpe, January 18, 2006
Cisco Systems Cisco IOS 11.x	A vulnerability has been reported in data that is received in CDP (Cisco Discovery Protocol) packets due to insufficient sanitization before displayed in the CDP status page, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	Cisco IOS CDP Status Page HTML Injection	Not available	iDefense Security Advisory, January 17, 2006
Clipcomm CPW-100E VOIP WIFI Phone 1.1.12, CP-100E VOIP WIFI Phone 1.1.60	A vulnerability has been reported on port 60023/tcp because connections are allowed to an undocumented debug service, which could let a	Clipcomm CWP-100/CP-100E Debug Service Unauthorized Access CVE-2006-0305	7	Security Focus, Bugtraq ID: 16289, January 17, 2006

	malicious user obtain unauthorized access. No workaround or patch available at time of publishing. There is no exploit code required.			
CounterPath eyeBeam	A buffer overflow vulnerability has been reported in the SIP Header data due to insufficient validation of the length of user-supplied strings prior to copying them into static process buffers, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept Denial of Service exploit, eyeBeam_dos.c, has been published.	CounterPath eyeBeam Remote Buffer Overflow	Not available	Security Focus, Bugtraq ID: 16253, January 16, 2006

CubeCart CubeCart 3.0.7 -pl1	Multiple Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of unspecified user-supplied input before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	CubeCart Multiple Cross-Site Scripting CVE-2006-0245	2.3	Security Focus, Bugtraq ID: 16259, January 16, 2006
Dual DHCP DNS Server Dual DHCP DNS Server 1.0	A buffer overflow vulnerability has been reported in the DHCP options field due to a boundary error, which could let a remote malicious user cause a Denial of Service or execution of arbitrary code. Windows Platform Fix Currently we are not aware of any exploits for this vulnerability.	Dual DHCP DNS Server DHCP Options Remote Buffer Overflow CVE-2006-0304	7	Security Tracker Alert ID: 1015495, January 17, 2006
EMC Legato Legato Networker 7.2.1	Several vulnerabilities have been reported: a remote Denial of Service vulnerability was reported when handling corrupted RPC packets due to an error; and a vulnerability was reported due to two unspecified errors, which could	EMC NetWorker Code Execution CVE-2005-3658 CVE-2005-3659	7 (CVE-2005-3658) 2.3 (CVE-2005-3659)	Secunia Advisory: SA18495, January 17, 2006

	let a remote malicious user obtain unauthorized access and execute arbitrary code. Hotfix Currently we are not aware of any exploits for these vulnerabilities.			
FAQ-O-Matic FAQ-O-Matic 2.711	Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of the '_duration,' 'file,' and 'cmd' parameters before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	Faq-O-Matic Cross-Site Scripting CVE-2006-0251	2.3	Security Focus, Bugtraq ID: 16251, January 16, 2006
Fog Creek Software FogBugz 4.0 29	A Cross-Site Scripting vulnerability has been reported in 'default.asp' due to insufficient sanitization of the 'dest' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. The vendor has released version 4.030 to address this issue; please	Fog Creek Software FogBugz Cross-Site Scripting CVE-2006-0194	2.3	Security Focus, Bugtraq ID: 16216, January 12, 2006

	contact the vendor for upgrades and further information. There is no exploit code required; however, a Proof of Concept exploit has been published.			
geoBLog geoBlog MOD_1.0	An information disclosure and SQL injection vulnerability was reported in 'viewcat.php' due to insufficient sanitization of the 'cat' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code and obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	GeoBlog SQL Injection & Information Disclosure CVE-2006-0249	2.3	Secunia Advisory: SA18504, January 16, 2006
GTP iCommerce Pty Ltd. iCommerce	Cross-Site Scripting vulnerabilities have been reported in 'index.php' due to insufficient sanitization of the 'subcat' and 'cat' parameters before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit	GTP iCommerce Multiple Cross-Site Scripting CVE-2006-0237	2.3	Security Focus, Bugtraq ID: 16255, January 16, 2006

	code required; however, Proof of Concept exploits have been published.			
HTMLtoNuke HTMLtoNuke	A file include vulnerability has been reported din 'htmltonuke.php' due to an input validation error, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	HTMLtoNuke Remote File Include CVE-2006-0308	7	Secunia Advisory: SA9275, January 17, 2006
IndexCOR ezDatabase 2.0 & prior	A vulnerability has been reported in 'vistorupload.php' due to insufficient sanitization of the 'db_id' parameter, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	EZDatabase Remote PHP Script Code Execution CVE-2006-0214	7	Security Focus, Bugtraq ID: 16237, January 14, 2006
Light Weight Calendar Light Weight Calendar 1.0	A vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'date' parameter, which could let a remote malicious user execute arbitrary php code. No workaround or	Light Weight Calendar PHP Code Execution CVE-2006-0206	7	Security Focus, Bugtraq ID: 16229, January 13, 2006

	patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.			
Marko microBlog 2.0 RC-10	Several vulnerabilities have been reported: SQL injection vulnerabilities were reported in 'index.php' due to insufficient sanitization of the 'month' and 'year' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a Cross-Site Scripting vulnerability was reported in the 'functions.php' script due to insufficient filtering of HTML code from the '[url]' BBCode tag before displaying the input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	microBlog SQL Injection & Cross-Site Scripting CVE-2006-0233 CVE-2006-0234	2.3 (CVE-2006-0233) 7 (CVE-2006-0234)	Security Tracker Alert ID: 1015496, January 17, 2006

MPN HP-180W VOIP WIFI Phone WE.00.17	An information disclosure vulnerability has been reported on port 9090/udp because connections are allowed to an undocumented service, which could let a malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required.	MPM HP-180W VOIP WIFI Phone Information Disclosure CVE-2006-0302	2.3	Security Focus, Bugtraq ID: 16285, January 17, 2006
Multiple Vendors Ubuntu Linux 5.10 powerpc, i386, amd64; Blender 2.40 alpha, 2.39, 2.37 a, 2.37, 2.30-2.35, 2.25 -2.28, 2.0 4	A buffer overflow vulnerability has been reported in 'get_bhead()' when parsing '.blend' files, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code. Ubuntu **Gentoo** A Proof of Concept exploit has been published.	Blender Buffer Overflow CVE-2005-4470	8	Ubuntu Security Notice, USN-238-2, January 06, 2006 **Gentoo Linux Security Advisory, GLSA 200601-08, January 13, 2006**

Netbula Anyboard 9.9.5 6	A Cross-Site Scripting vulnerability has been reported in the 'anyboard.cgi' script due to insufficient sanitization of the 'tK' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Netbula Anyboard Cross-Site Scripting CVE-2006-0247	2.3	Secunia Advisory: SA18469, January 16, 2006
Oracle Corporation JD Edwards EnterpriseOne 8.x, Oracle Application Server 10g, Collaboration Suite Release 1 & Release 2, Database 8.x, Database Server 10g, Developer Suite 10g, E-Business Suite 11i, Enterprise Manager 10.x, Oracle9i Application Server, Oracle9i Database Enterprise Edition, Oracle9i Database Standard Edition, Oracle9i Developer Suite, PeopleSoft Enterprise Portal 8.x	82 vulnerabilities and security issues have been reported in various Oracle products, which could lead to information disclosure, arbitrary files overwritten, and arbitrary SQL code injection. patch information An exploit would not be required for some of these issues.	Oracle January Security Update CVE-2005-2371 CVE-2005-2378 CVE-2006-0256 through CVE-2006-0291	3.3 (CVE-2005-2371) 3.3 (CVE-2005-2378) 7 (CVE-2006-0256 through CVE-2006-0271) 7 (CVE-2006-0272 through CVE-2006-0278) 4.9 (CVE-2006-0279 & CVE-2006-0280) 7 (CVE-2006-0281 through CVE-2006-0291)	Security Focus, Bugtraq ID: 16287, January 17, 2006 US-CERT VU#545804 Technical Cyber Security Alert TA06-018A
PayPal PHP Toolkit PayPal PHP Toolkit 0.50	Several vulnerabilities have been reported: a vulnerability was reported due to the insecure	PHP Toolkit for PayPal Payment Bypass & Transaction Exposure CVE-2006-0201	2.3 (CVE-2006-0201) 3.3 (CVE-2006-0202)	Secunia Advisory: SA18444, January 13, 2006

	storage of payment information in the 'logs' directory, which could let a remote malicious user obtain sensitive information; and a vulnerability was reported in the 'ipn_success.php' script due to insufficient verification of the origin of payment information, which could let a remote malicious user write a successful payment even when no payment occurred. No workaround or patch available at time of publishing. There is no exploit code required.	CVE-2006-0202		
pdfdirectory pdfdirectory 0.2.2-0.2.11	Several vulnerabilities have been reported: SQL injection vulnerabilities have been reported due to insufficient sanitization of unspecified input, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability was reported because sensitive data is stored in plaintext, which could let a remote malicious user obtain arbitrary users' passwords. Updates available There is no exploit code required.	PDFDirectory SQL Injection CVE-2006-0313 CVE-2006-0314	7 (CVE-2006-0313) 7 (CVE-2006-0314)	Secunia Advisory: SA18459, January 17, 2006

PHP Fusebox PHP Fusebox 4.0.6	A Cross-Site Scripting vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'fuseaction' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PHP Fusebox Cross-Site Scripting CVE-2006-0242	4.7	Security Focus, Bugtraq ID: 16274, January 17, 2006
PHP PHP 5.1.1, 5.1	Several vulnerabilities have been reported: a vulnerability was reported due to insufficient of the session ID in the session extension before returning to the user, which could let a remote malicious user inject arbitrary HTTP headers; a format string vulnerability was reported in the 'mysqli' extension when processing error messages, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported due to insufficient sanitization of unspecified input that is passed under certain error conditions, which could let a remote malicious user	Multiple PHP Vulnerabilities	Not available	Secunia Advisory: SA18431, January 13, 2006

	execute arbitrary HTML and script code. PHP There is no exploit code required.			
phpXplorer phpXplorer 0.9.33	A Directory Traversal vulnerability was reported in 'workspaces.php' due to insufficient sanitization of the 'sshare' parameter, which could let a remote malicious user obtain sensitive information. *Note: This vulnerability has been disputed.* No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	phpXplorer Directory Traversal CVE-2006-0244	2.3	Secunia Advisory: SA18518, January 17, 2006
PowerPortal PowerPortal 1.3 b, 1.3, 1.1 b	Multiple vulnerabilities have been reported: a path disclosure vulnerability was reported in error pages when invalid input is submitted or when scripts are accessed directly, which could let a remote malicious user obtain sensitive information; a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of various parameters in certain unspecified modules, which	PowerPortal Multiple Vulnerabilities CVE-2004-0662 CVE-2004-0663 CVE-2004-0664	3.3 (CVE-2004-0662) 10 (CVE-2004-0663) 3.3 (CVE-2004-0664)	Security Focus, Bugtraq ID: 16279, January 17, 2006

	could let a remote malicious user execute arbitrary HTML and script code; and a Directory Traversal vulnerability was reported in the 'gallery' module due to insufficient validation of the 'files' parameter, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.			
SMBCMS SMBCMS 2.1	A Cross-Site Scripting vulnerability has been reported in the site search feature due to insufficient sanitization of the 'text' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required	SMBCMS Cross-Site Scripting CVE-2006-0243	2.3	Secunia Advisory: SA18454, January 17, 2006

Sun Microsystems, Inc. Java JDK 1.5.x, Java JRE 1.3.x, 1.4.x, 1.5.x / 5.x, Java SDK 1.3.x, 1.4.x	Several vulnerabilities have been reported: a vulnerability was reported due to an unspecified error, which could let a malicious untrusted applet read/ write local files or execute local applications; three unspecified vulnerabilities were reported with the use of 'reflection' APIs error, which could let a malicious untrusted applet read/write local files or execute local applications; and a vulnerability was reported in the Java Management Extensions (JMX) implementation, which could let a malicious untrusted applet read/ write local files or execute local applications. Upgrade information Sun Sun IBM **SuSE** **Gentoo** Currently we are not aware of any exploits for these vulnerabilities.	Sun Java Runtime Environment Security Bypass CVE-2005-3904 CVE-2005-3905 CVE-2005-3906 CVE-2005-3907	9 (CVE-2005-3904) 9 (CVE-2005-3905) 9 (CVE-2005-3906) 9 (CVE-2005-3907)	Sun(sm) Alert Notifications Sun Alert ID: 102003, 102017, & 102050, November 28, 2005 US-CERT VU#974188, VU#355284, VU#931684 IBM Technote, December 16, 2005 **SUSE Security Summary Report, SUSE-SR:2006:001, January 13, 2006** **Gentoo Linux Security Advisory, GLSA 200601-10, January 16, 2006**
Tank Logger TankLogger 2.4	SQL injection vulnerabilities have been reported in 'livestock.php' due to insufficient sanitization of the 'tank_id' parameter and in	TankLogger SQL Injection CVE-2006-0209	7	Security Focus, Bugtraq ID: 16228, January 13, 2006

	'showInfo.php' due to insufficient sanitization of the 'tank_id' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. A Proof of Concept exploit, EV0026.txt, has been published.			
thinkfactory Ultimate Auction 3.67	A Cross-Site Scripting vulnerability has been reported 'item.pl' due to insufficient sanitization of the 'item' parameter and in 'itemlist.pl' due to insufficient sanitization of the 'category' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	Ultimate Auction Cross-Site Scripting CVE-2006-0217	2.3	Secunia Advisory: SA18477, January 16, 2006
TopCMM Computing 123 Flash Chat Server 5.1, 5.0	A file creation vulnerability has been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user create/overwrite arbitrary files. Update available There is no exploit code required.	123 Flash Chat Server Remote Arbitrary File Creation CVE-2006-0223	2.3	Security Focus, Bugtraq ID: 16235, January 13, 2006

Tux Paint Tux Paint 0.9.15 b, 0.9.14	A vulnerability has been reported in the 'tuxpaint-import.sh' script due to the insecure creation of temporary files, which could let a malicious user obtain elevated privileges. Debian Ubuntu There is no exploit code required.	Tux Paint Insecure Temporary File Creation CVE-2005-3340	4.9	Debian Security Advisory, DSA-941-1, January 16, 2006 Ubuntu Security Notice, USN-243-1, January 16, 2006
WebMobo WBNews 1.1 .0	An HTML injection vulnerability has been reported in 'comments.php' due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	WebMobo WBNews HTML Injection CVE-2006-0241	2.3	Security Focus, Bugtraq ID: 16277, January 17, 2006
White Angle White Album 2.5	An SQL injection vulnerability has been reported in 'pictures.php' due to insufficient sanitization, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	White Album Pictures.PHP SQL Injection CVE-2006-0235	7	Security Focus, Bugtraq ID: 16247, January 16, 2006
Wordcircle Wordcircle 2.17	Several vulnerabilities have been reported: a	wordcircle Script Insertion & SQL Injection	2.3 (CVE-2006-0204)	Secunia Advisory: SA18440, January 13, 2006

	vulnerability was reported in the course name field when adding a new course due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code; and an SQL injection vulnerability was reported due to insufficient sanitization of the password field when logging, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, exploitation details, EV0027.txt and EV0028.txt, have been published.	CVE-2006-0204 CVE-2006-0205		

[back to top]

Wireless Trends & Vulnerabilities

This section contains wireless vulnerabilities, articles, and malicious code that has been identified during the current reporting period.

- Cisco Aironet Wireless Access Point ARP Remote Denial of Service: A remote Denial of Service vulnerability has been reported when handling an excessive number of ARP requests.
- Toshiba Bluetooth Information Disclosure. An input validation vulnerability has been reported in Toshiba Bluetooth that could let remote malicious users to disclose information.
- CounterPath eyeBeam Remote Buffer Overflow: A remote buffer overflow vulnerability was been reported in the SIP Header data.
- MPM HP-180W VOIP WIFI Phone Information Disclosure: An information disclosure vulnerability has been reported on port 9090/udp.
- ACT P202S VOIP WIFI Phones Multiple Remote Vulnerabilities; Several vulnerabilities have been reported which could let a remote malicious user cause a Denial of Service, obtain sensitive information and bypass security restrictions.
- Clipcomm CWP-100/CP-100E Debug Service Unauthorized Access: A security issue has been reported which could let a malicious user obtain sensitive information, manipulate certain information, and bypass security restrictions.
- Simple wireless flaw revealed: According to information related at ShmooCon, a feature in the way Windows

handles wireless connections could be exploited to gain access. The issue involves ad-hoc wireless connections, which are automatically created when the laptop is powered up and no infrastructure access points are available.
- Prepare Your Company For WiMax: WiMax, the wireless technology that provides broadband connections over long distances, is becoming available in an increasing amount of cities. According to an analyst for Datecon, Inc, when WiMax becomes available locally it can effectively replace a company's T-1 line and provide better connections inside and outside the company.

[back to top]

General Trends

This section contains brief summaries and links to articles which discuss or present information pertinent to the cyber security community.

- The number of 'classic' viruses dropped dramatically in 2005 compared to worms and Trojans, reports Panda Software: According to data released by PandaLabs, less than one percent of the new threats detected in 2005 were viruses, however, threats like Trojans and worms still had a significant presence compared to the previous year. The new threats detected in 2005 included: 42 percent Trojans, 26 percent bots, 11 percent backdoor Trojans, 8 percent dialers, 6 percent worms and 3 percent were types of adware/spyware.
- Exploit for Vulnerability in VERITAS NetBackup Volume Manager Daemon: US-CERT is aware of a public exploit for a vulnerability in VERITAS NetBackup Volume Manager Daemon (vmd).
- Malicious Website Exploiting Sun Java Plug-in Vulnerability; US-CERT is aware of an active malicious website that exploits a vulnerability in the Sun Java JRE.
- Mac users 'too smug' over security: MacOS may not have the gaping holes that let viruses spread,but worms, spyware and keyloggers are out there. They can't spread as easily, and most would only be installed by a careless user clicking "Accept" on a dodgy install dialog, but the regular stream of security fixes from Apple's software update service makes it clear that there are real dangers.
- Phishers casts their nets wider: According to the Anti-Phishing Working Group (APWG) a sharp rise in the number of phishing attacks, combined with an increased sophistication among attackers was reported. In its monthly report for November 2005 the APWG said that reported attacks grew to 16,882 from 15,820, the third month of growth after a slowdown over the summer.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trend	Date	Description
1	Netsky-P	Win32 Worm	Stable	March 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it

					finds when scanning the hard drives and mapped drives. The worm also tries to spread through various file-sharing programs by copying itself into various shared folders.
2	Mytob-GH	Win32 Worm	Stable	November 2005	A variant of the mass-mailing worm that disables security related programs and allows other to access the infected system. This version sends itself to email addresses harvested from the system, forging the sender's address.
3	Netsky-D	Win32 Worm	Stable	March 2004	A simplified variant of the Netsky mass-mailing worm in that it does not contain many of the text strings that were present in NetSky.C and it does not copy itself to shared folders. Netsky.D spreads itself in e-mails as an executable attachment only.

4	Zafi-B	Win32 Worm	Stable	June 2004	A mass-mailing worm that spreads via e-mail using several different languages, including English, Hungarian and Russian. When executed, the worm makes two copies of itself in the %System% directory with randomly generated file names.
5	Sober-Z	Win32 Worm	Stable	December 2005	This worm travels as an email attachment, forging the senders address, harvesting addresses from infected machines, and using its own mail engine. It further download code from the internet, installs into the registry, and reduces overall system security.
6	Lovgate.w	Win32 Worm	Stable	April 2004	A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and

					through peer-to-peer networks. Attempts to access all machines in the local area network.
7	Mytob.C	Win32 Worm	Stable	March 2004	A mass-mailing worm with IRC backdoor functionality which can also infect computers vulnerable to the Windows LSASS (MS04-011) exploit. The worm will attempt to harvest email addresses from the local hard disk by scanning files.
8	Zafi-D	Win32 Worm	Stable	December 2004	A mass-mailing worm that sends itself to email addresses gathered from the infected computer. The worm may also attempt to lower security settings, terminate processes, and open a back door on the compromised computer.
9	Mytob-BE	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that utilizes an IRC backdoor, LSASS vulnerability,

					and email to propagate. Harvesting addresses from the Windows address book, disabling anti virus, and modifying data.
10	Mytob-AS	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that disables security related programs and processes, redirection various sites, and changing registry values. This version downloads code from the net and utilizes its own email engine.

Table updated January 17, 2006

[back to top]

Last updated January 19, 2006